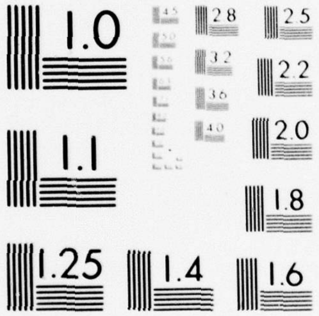
AD-A071 719 GEORGIA INST OF TECH ATLANTA SCHOOL OF INFORMATION A--ETC F/G 12/1
SOME CONNECTION BETWEEN MATHEMATICAL LOGIC AND COMPLEXITY THEOR--ETC(U)
APR 79 R A DEMILLO, R J LIPTON DAAG29-76-G-0338
UNCLASSIFIED GIT-ICS-79/01 ARO-14690.9-EL NL

| OF |

AD
A071719

END
DATE
FILMED
8-79
DDC



MICROCOPY RESOLUTION TEST CHART

ARO 14690.9-EL

12

LEVEL II

See back page for 1473

SEAL OF THE GEORGIA INSTITUTE OF TECHNOLOGY 1885

School of

Information and Computer Science

GEORGIA INSTITUTE OF TECHNOLOGY

79 07 24 065

GIT-ICS-79/01 12

Some Connections Between Mathematical Logic and Complexity Theory

Richard A. DeMillo *

Richard J. Lipton **

APRIL 1979

* Georgia Institute of Technology

** University of California, Berkeley
and Yale University

SOME CONNECTIONS BETWEEN MATHEMATICAL LOGIC AND COMPLEXITY THEORY[†]

Richard A. DeMillo
School of Information and Computer Science
Georgia Institute of Technology
Atlanta, GA 30332

Richard J. Lipton
Computer Science Division
University of California, Berkeley
Berkeley, CA 94720

and

Department of Computer Science
Yale University
New Haven, CT 06520

[†] This work was supported in part by the US Army Research Office Grant No. DAAG29-76-G-0024 and by National Science Foundation Grants No. MCS-78-81486 and No. MCS-78-07379. Our work was also facilitated by the use of Theory Net, NSF Grant No. MCS-78-01689

I. Introduction

However difficult the fundamental problems of theoretical computer science may seem, there is very little to suggest that they are anything more than knotty combinatorial problems. So, when we look for reasons for our inability to resolve P = NP and related questions, we most likely find them dealing with a lack of understanding of particular computational problems and their lower bounds. This is the sense of Hopcroft's prediction: "...within the next five years, nobody will prove that any of these problems takes more than let's say n^2 time. I think that's a reasonably safe conjecture and it also illustrates how little we know about lower bounds." [MT]. Hopcroft's guess is uncanny in its accuracy -- after six years and considerable effort by many researchers, his conjecture remains unchallanged.

The results in this paper offer a possible explanation for our failure to resolve these problems. Roughly, the main result of the sequel links lower bounds and a branch of mathematical logic known as model theory. In particular, we prove that the existence of nonpolynomial lower bounds is equivalent to the existence of nonstandard models of a sizable fragment of arithmetic. Since these are deep logical issues and there are very few techniques for handling them, and since the nonstandard models in question are noneffective, it seems plausible that this linking of complexity theory and logic explains our failure to obtain nontrivial lower bounds.

One of the aims of mathematical logic is to clarify the relation between mathematical theories and their interpretations -- or models. In logic, a theory is simply a collection of statements and all of their logical consequences, that is, a collection of (nonlogical) axioms closed under the relation "$\vdash$".

Models are the structures in which theories are interpreted.

Plane geometry is such a mathematical theory. In antiquity, the relation between Euclidean geometry and its models was considered obvious, and this relationship was even further clarified by the arithmetization of geometry. It was therefore a shock to the mathematical world when, in 1868, Beltrami announced that geometry can have more than one model -- a very strange one at that since in his model the parallel postulate is false. Since the parallel postulate is certainly true in the standard model of geometry, its negation is not provable -- the parallel postulate is consistent with Euclidean geometry. On the other hand, since the negation of the parallel postulate is also true in a (nonstandard) model, its negation (i.e., the parallel postulate itself) is not provable. More recently, Cohen [Co] proved that both the axiom of choice and generalized continuum hypothesis cannot be proved from the remaining axioms of set theory -- Cohen introduced a radically new concept called forcing to construct nonstandard models with prescribed properties. The first such result for formal arithmetic was obtained by Paris and Harrington [PH]. They proved that a modest generalization of the finite Ramsey theorem of combinatorics is not decided by Peano arithmetic. Sheperdson [Sh] discusses the unprovability of induction schemes and such statements as Fermat's Last Theorem, for the case n = 3, from weak fragments of arithmetic.

This property of statements of a theory is called independence: a statement is independent from a theory T if the statement cannot be proved or disproved within T. Of course, Gödel proved that every sufficiently powerful theory must leave infinitely many statements unresolved in this way. In current terminology, however, a qualitative distinction is usually drawn between formal undecidability and interesting independence theorems. In the

Gödel-style formal undecidability theorems, one explicitly formulates a diagonalizing statement and using the properties of the axiom system in question, encodes that statement as a formal statement of the theory. In independence results whatever diagonalization is present in the proof, is well-hidden. One begins with a fixed (true) formal statement -- whose formalization has not been obtained with a knowledge of the axioms to be used -- and using model theoretic techniques, shows an interpretation in which the statement fails to hold (cf. [DL] for a survey of these results). Therefore, independence results seem to exhibit the following characteristics.

(1) There is no direct diagonalization. That is, the statements whose independence is to be proved do not refer explicitly to, say, halting computations.

(2) The independent statements are interesting in their own right. In set theory, for instance, independent statements often represent useful infinitary combinatorial principles.

(3) The independence of a statement is sensitive to the underlying theory. In formal undecidability results one can add additional axioms to the theory, encode the independent statement for the new theory and retain its undecidability. In interesting independent theorems, however, the independence of the statement from a set of axioms characterizes the power of the axioms; changing the underlying theory by adding more axioms decides the statement in the expanded theory.

Except for the discussion of Hopcroft and Hartmanis [HH] and the results of Lipton [Li], we are aware of no other results that relate the basic issues of complexity theory to independence or nonstandard models. The impact of our results is that proving lower bounds on certain computational problems is as hard as showing that a certain true sentence is independent from a powerful theory. In particular, we show that for certain S, $S \not\in P$ (i.e., S is intractible) exactly when a particular true sentence Δ_S related to S must be false in a nonstandard model of arithmetic. Furthermore, this model must be noneffective. The various proofs of this result yield existential proof techniques for showing that problems are solvable in polynomial time. An interesting aspect of this result is that it apparently does not generalize much beyond polynomial time computation. That is, it does not relativize in any obvious way, nor is it possible to formally substitute many other time classes for P in the statement of the theorem.

II. Definitions

The definitions from complexity theory are standard [BL]. P denotes the set of problems solvable in deterministic polynomial time. NP denotes the problems solvable in nondeterministic polynomial time, and coNP denotes the set of problems whose complements lie within NP. The inclusions

$$P \subseteq NP \cap coNP \subseteq NP$$

are obvious. Although it is widely believed that both inclusions are strict, the results to be quoted below are interesting even if, say, $P = NP \cap coNP$. We will return to this point later.

Our logical notation is standard (see [Ba]). Our language is any acceptable first order language with arithmetical symbols and quality. We use $\forall$ for universal quantification and $\exists$ for existential quantification. Among other symbols, x,y,z are used for variables, and the infix symbols

$+$ and $\times$ and $\dot{-}$ are used for addition and multiplication and subtraction, suc and pred for the successor and predecessor functions, and 0 for the constant zero.

Let T be a set of formulas, then $T \vdash \phi$ indicates that ϕ is a logical consequence of T. A *theory* is simply the set of formulas which are logical consequences of T. Since the set of theorems of the theory is uniquely characterized by T, we identify the two. A theory is consistent if $0=1$ is not among its theorems. A formula ϕ is independent of the theory if neither ϕ nor $\sim\phi$ is a theorem. If T is a theory, $T+\phi$ denotes the result of adjoining ϕ as an axiom. Thus ϕ is independent of T if both $T+\phi$ and $T+\sim\phi$ are consistent. A model of a theory T is an interpretation of the individuals, functions and relations of the underlying language such that each $\phi \in T$ is true. A set of formulas has a model if and only if it is consistent. In addition to this basic fact, we will use the

Compactness Theorem [BS]: Let T be a set of formulas. T has a model iff every finite subset of T has a model.

We will deal with a subtheory of (complete) arithmetic. Of course the *standard* model of this theory is the integers $N = \{0,1,2,...\}$ with the remaining symbols interpreted in the obvious way. Any model *N (with + interpreted as *+, etc.) which is not isomorphic to N is said to be *nonstandard.* Since *N may be uncountable it is not surprising that nonstandard models of arithmetic can exist. Skolem [SK], however, showed that *countable* nonstandard models are possible. We will discuss these more fully in Section IV. For now it will be sufficient to note that if *N is a countable nonstandard model of arithmetic *N-N consists of *nonstandard* objects which are infinite relative to N; i.e., if $a \in$ *N-N, $a > n$, for each $M \in N$. Henceforth

*N (or $*N_0, *N_1$) always denotes such a model.

We will now define a particular theory PT. The language for PT includes symbols for all the functions and predicates which are countable in polynomial time. The axioms of PT are all true sentences of the form

$$(\exists x)(\forall y)A(x,y),$$

where A is quantifier-free (as usual x and y may denote several occurrences of bound variables). A formula with such a quantifier is called an EA formula. Similarly an AE formula contains the quantifier prefix $\forall\exists$. The theory PT is quite powerful. It includes the theory studied by Skolem [Skl] -- which he felt represented an important part of constructive number theory. Hilbert, Herbrand, Kreisel and Scott [Sc] have also studied systems much weaker than PT (Sh]. Perhaps more relevant to our discussion, the PV system of Cook [Ck1, Ck2] is also weaker than PT. The axioms of PT include all the recursive equations that define the functions and predicates included in PT. Moreover, PT contains the induction axiom

$$A(0) \wedge (\forall x)[A(x) \rightarrow A(x+1)] \rightarrow (\forall y)A(y). \qquad (*)$$

where A is a quantifier-free. To see this just note that (*) is equivalent to

$$(\exists x)(\forall y)[\neg A(0) \vee (A(x) \wedge \neg A(x+1)) \vee A(y)].$$

For model-theoretic purposes the axioms PT can be replaced by their universal members without changing the degree of the theory: both axiomatizations are equivalent. The theory which Skolem studied can be formed by (*) and the recursive definitions of the functions successor, addition, multiplication, subtraction and integer division. Cook's PV theory is related to PT, but notice that PT is not even recursively enumerable (inclusion of an axiom depends upon its truth), so that PT is a vastly more powerful theory. Indeed it is not obvious how to deal with independence from PT using other than model-theoretic techniques -- since PT is not recursively enumerable, it is not clear how diagonalization can work at all!

III. Main Result

Our main result is that the intractability of any $S \in NP \cap coNP$ is equivalent to the existence of a nonstandard model for PT in which a certain sentence Δ_S, related to S, fails; i.e., PT + $\sim\Delta_S$ is a consistent theory.

Let S be fixed and let $A(x,y)$, $B(x,y)$ be defined as follows:

$$(\exists y)A(x,y) \text{ iff } x \in S,$$

and

$$(\exists y(B(x,y) \text{ iff } x \notin S.$$

Now form $\Delta_S(A,B)$:

$$\Delta_S(A,B) = (\forall x)[(\exists y)A(x,y) \vee (\exists z)B(x,z)]$$

Notice that, when interpreted in N, $N \models \Delta_S(A,B)$ since in N

$$\Delta_S(A,B) \leftrightarrow (\forall x)(x \in S \vee x \notin S).$$

Theorem. Let $S \in NP \cap coNP$. Then the following statements are equivalent:

(1) $S \in P$.

(2) $PT \vdash \Delta_S(A,B)$, for some A,B in the language of PT.

Proof of (1) ⇒ (2): If $S \in P$, there are polynomial time predicates A,B so that $x \in S$ iff $A(x)$ and $x \notin S$ iff $B(x)$.

Hence

$$(\forall x)[(\exists y)A(x) \vee (\exists z)B(x)]$$

is an axiom of PT.

□

Proof of (2) ⇒ (1):

We will present three proofs of the converse. What is needed in all three cases is to pass from PT $\vdash \Delta_S(A,B)$ to a true formula

$$(\forall x)(\bigvee_{i=1}^{n} A(x,f_i(x)) \vee \bigvee_{i=1}^{m} B(x,g_i(x)))$$

where the terms f_i, g_i are in the language of PT. Hence $x \in S$ is decided by checking

$$\bigvee_{i=1}^{n} A(x,f_i(x)) \qquad (3)$$

and

$$\bigvee_{i=1}^{m} B(x,g_i(x)) \qquad (4)$$

If (3) is true $x \in S$ and if (4) is true $x \notin S$, and since all terms and predicates are polynomial time computable, $S \in P$.

Proof A:

Let $(\forall x)(\exists y)\Gamma(x,y)$ denote $\Delta_S(A,B)$, so that PT $\vdash (\forall x)(\exists y)\Gamma(x,y)$, and suppose that

$$\text{PT} \not\vdash (\forall x)(\bigvee_{i=1}^{n} \Gamma(x,f_i(x)), \qquad n=1,2,\ldots$$

where $f_1, f_2, \ldots$ are terms of PT. Define the theory T* by

$$T^* = PT + \sim\Gamma(c,f_1(c)) + \ldots + \sim\Gamma(c,f_n(c)) + \ldots$$

where c is a new constant, not appearing in PT. We first claim that T* is consistent, for if not

$$PT + \sim\Gamma(c,f_1(c)) + \ldots + \sim\Gamma(c,f_m(c)) \vdash 0=1$$

by compactness and hence

$$PT \vdash \bigvee_{i=1}^{n} \Gamma(c,f_i(c))$$

which implies

$$PT \vdash (\forall x) \bigvee_{i=1}^{m} \Gamma(x,f_i(x)),$$

establishing the claim. Choose any model M for T* and let M_c be the submodel generated by c. Since PT is open, $M_c \models PT$ and thus $M_c \models (\exists y)\Gamma(c,y)$. But by our choice of c, $M_c \models (\forall y)\sim\Gamma(c,y)$. S ε P now follows as described above.

□

Proof B:

We need to recall the following fact, often called the Kleene-Herbrand-Gentzen Theorem [Kl].

Lemma If T is a consistent collection of EA formulas and $T \vdash (\forall x)(\exists y)\phi(x,y)$ where ϕ is open, then for some terms over the terms of T, their compositions and definition by cases, say $f_1, \ldots, f_m$,

$$\bigvee_{i=1}^{m} \phi(x,f_i(x))$$

is true.

Roughly speaking, this allows us to make the existential quantifiers explicit in a quite constructive fashion. Without the restriction on T the lemma is easily seen to be false. Since PT satisfies the hypothesis for T and $\Delta_S(A,B)$ is AE, $S \in P$ follows by (3), (4) as described above.

□

Proof C:

The application of the Kleene-Herbrand-Gentzen Theorem can be replaced by an application of the "pure" Herbrand Theorem [Stl] as in Proof B to conclude PT $\vdash$ "$S \in P$".

□

Notice that Proof A is nonconstructive and involves compactness arguments. The provability of $\Delta_S(A,B)$ in this setting constitutes a "pure" existence proof for polynomial time algorithms. The provability of $\Delta_S(A,B)$ in the setting of Proofs B and C constitutes a constructive existence proof for polynomial time algorithms. (The apparent simplicity of Proof B compared to Proof A lies in the great power of Herbrand's Theorem, which has played a basic role in various consistency proofs in logic. The proof of Herbrand's Theorem is based on a very careful analysis of how T can prove $(\forall x)(\exists y)\phi(x,y))$. However, the running times of polynomial time algorithms produced in this way may be very bad indeed. In fact, the best known bound is of order

$$n^{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}} \tag{5}$$

where the depth of nesting of the stack of 2's is bounded by the number of inferences in the shortest proof of $\Delta_S(A,B)$ in PT. These upper bounds are the best known to logicians, although the lower bound literature is very sparse (Statman has obtained this polynomial as a lower bound [St] although for a theory much less relevant to complexity theorists). It has been often noticed that, although there are problems with very large polynomial running times, the only naturally occuring problems in P have "small" polynomial complexity. This gap has helped to sustain a certain feeling that membership in P is sufficient for computational tractability. If indeed the polynomial bounds (5) cannot be locally reduced, this is compelling evidence that P is much too extensive

This theorem above does not apply to arbitrary complexity classes. It is apparently rather highly specialized for polynomial-like complexity classes. At concrete levels, the theorem can be made to work for the following complexity classes:

$2^{\text{poly-log}}$

linear

$n^{1+\varepsilon}$

$\bigcup_k n\log^{(k)} n$

How about those problems for which lower bound proofs have already been supplied?[†] The theorem does not hold for any elementary lower bound (functions which consist of bounded nestings of exponentials do not have the

[†] This issue was raised by R. E. Tarjan.

closure properties required by Herbrand's Theorem). On the other hand, the Δ_S sentence for those sets which have provable nonelementary lower bounds [MS] are false in the standard model of T, and so the issue of independence does not even arise for those problems. In short, the theorem cannot apply to a class of lower bounds F if the functions in F are not closed under compositon and definition by cases, or if determinism and nondeterminism are not distinguished at complexity F.

By identical arguments we can show that PT is also related to "P = NP." Let us say that a theory T can verify that NP is closed under complements if for $S \in NP$

$$T \vdash \text{"}S \in coNP.\text{"}$$

Corollary. PT can verify that NP is closed under complements iff P = NP.

By "checking" the theorem against the well-known problems which lie in $NP \cap coNP$ (e.g., Primes, Linear Programming, Breaking Public Key Cryptosystem [Ri]), a great deal of information can be obtained about the nonstandard models whose existence is so intimately connected to lower bounds. We have the corollaries:

Corallary. If Primes is not in P, then there is a nonstandard model of PT in which primes need not have primitive roots [Pr].

Corollary. If Linear Programming is not in P, then there is a nonstandard model of PT in which for some point y and some point-set X whose convex hull does not contain y, there is no separating hyperplane through y [Do].

Since both of these corollaries negate properties which hold in the standard integers, it is difficult to imagine the models in which they fail.

Moreover, the classical techniques for constructing nonstandard models do not work at the simple level of $\Delta_S(A,B)$. For example, forcing is a technique that can be applied to formulas very high in the analytical hierarchy [Bu]. It is generally acknowledged by logicians that there are few techniques for constructing such nonstandard models, yet the theorem cited above asserts that a byproduct of any lower bound proof is an existence proof for such nonstandard models.

Finally, we note that although we are unable to extend these results to Peano Arithmetic, we can extend the theory PT slightly to include theories with the property that all terms which grow slowly are easy to compute. Thus we have corresponding independence results for theories of +, × and polynomially honest functions. For instance, suitable theories are theories of

$$+,\times,x! \qquad \text{and} \qquad +,\times,x^{y+1}$$

IV. Nonstandard Models

In this section we will describe a result, due to R. Solovay, showing that from the standpoint of constructing nonstandard models the theory PT is almost as strong as Peano Arithmetic (PA, for short). We begin with a digression on the nature of nonstandard models of PA and fragments of arithmetic.

The classical observation of Skolem was that a countable nonstandard model of PA could be obtained simply by applying compactness to the set of formulas

$$PA + (a>0) + (a>1) + (a>2) + \dots$$

It is consistent to assume, then, that there exists a "nonstandard object" a which is greater than all standard integers. Such a model $^*N$ contains N as an initial segment and has an ordering $^*\leq$ extending $\leq$ to $^*N-N$. The global structure of $^*N$ is remarkable. Define for $x,y \in {}^*N$ $x \equiv y$ to mean that x and y differ by a standard integer, i.e., for some $n \in N$:

$$x{*}{-}y = n \qquad \text{or} \qquad y{*}{-}x = n.$$

$^*N/\equiv$ is a set of equivalence classes called blocks (each is order isomorphic to N). N is a block. Also $^*\leq$ totally orders blocks like the rationals (i.e., blocks are densely ordered). Nonstandard integers cannot be described by formulas of PA and any formula true of infinitely many integers must also hold at some $b \in {}^*N - N$.

Nonstandard models for fragments of arithmetic also contain infinite, nonstandard objects but may have vastly simpler structure. Consider the (infinite) axiom system: for all $n, m \in N$,

$\mathrm{suc}^m(0)+0 = \mathrm{suc}^m(0)$,

$\mathrm{suc}^m(0)+\mathrm{suc}(\mathrm{suc}^m(0)) = \mathrm{suc}(\mathrm{suc}^{m+n}(0))$,

$\mathrm{suc}^n(0)\times 0 = 0$,

$\mathrm{suc}^n(0)\times\mathrm{suc}(\mathrm{suc}^m(0)) = \mathrm{suc}^n(0)\times\mathrm{suc}^m(0)+\mathrm{suc}^n(0)$,

$\mathrm{suc}^n(0) \neq \mathrm{suc}^m(0)$, for $m \neq n$,

$(\forall x)(x \leq \mathrm{suc}^m(0) \leftrightarrow \bigvee_{0\leq i\leq m} x = \mathrm{suc}^i(0))$,

$(\forall x)(x \leq \mathrm{suc}^m(0) \vee \mathrm{suc}^m(0) \leq x)$.

A nonstandard model for this theory is

$^*N = N \cup \{\omega\}$, $w \notin N$ with $^*\mathrm{suc}(\omega) = 0$,

$^*\mathrm{suc}(m) = \mathrm{suc}(m)$ for all $m \in N$ and $^*+$, $^*\times$ defined by the following tables

$*+$	$x=\omega$	$x\varepsilon N$
$y=\omega$	ω	ω
$y\varepsilon N$	ω	$x+y$

$*\times$	$x=\omega$	$x\varepsilon N$
$y=\omega$	0	0
$y\varepsilon N$	0	$x\times y$

As another example, take the open theory of suc,pred,+,× and $\dot{-}$ together with the induction axiom

$$A(0) \wedge (\forall x)[A(x) \rightarrow A(suc(x)] \rightarrow A(x), \qquad A \text{ open}$$

A nonstandard *N consists of all nonnegative elements $Q(t)$ of the ring of polynomials

$$\sum_{i=0}^{p-1} a_{p-1} t^{p-i/q} + b,$$

Where $b,p,q \varepsilon N$, $a_i \varepsilon \mathbb{R}$ are algebraic and $Q(t) \; {*\leq} \; Q'(t)$ is determined by letting $t \rightarrow \infty$.

This model is quite important since it contains a nonstandard element $t\sqrt[3]{2}$ such that

$$(t\sqrt[3]{2})^3 = t^3 + t^3,$$

so that Fermat's Last Theorem for m=3 fails in *N (see [Sh] for details).

An important aspect of these weak fragments of arithmetic is that they can have "effective" nonstandard models, such as the two models described above. That is, there is a recursive definition of *+ and *x in terms of an enumeration of the universe.

The possibility of independence from PT would be less intriguing if PT turned out to be one of these weak fragments. That is, if a *N such that $*N \models \sim\Delta_S(A,B)$ could be found in which *+ and *x could be explicitly defined by finite combinatorial means. In fact, PT has no effective nonstandard models, so that proofs of lower bounds are necessarily connected with the existence of nonrecursive objects. We now sketch Solovay's proof of this fact.

We first need the corresponding result for PA, known as Tannenbaum's Theorem (cf. [Co] and [EK]): let $*N$ be a nonstandard model of PA; then at least one of $*+$ and $*x$ must be nonrecursive. The key idea of the proof is to find a nonstandard object y which effectively encodes the infinite membership information regarding a nonrecursive set S. This can be done as follows. It is possible in PA to define an RE nonrecursive set S. In $*N$, S is $*S$. If p_i is the i^{th} prime in $*N$, the Chinese Remainder Theorem holds for the system

$$y \equiv b_i \bmod p_i,\ P_i < c \ \varepsilon\ {}^*N \qquad (6)$$

Let $c\ \varepsilon\ {}^*N-N$ and define the b_i in (6) by:

$$b_i = \begin{cases} 0, \text{ if } i \ \varepsilon\ S \\ 1, \text{ if } i \notin S \end{cases}$$

Information in y about $*S$ is decoded as follows: search $*N$ for a z such that $p_n z = y$ (i.e., $n\ \varepsilon\ {}^*S$) or $p_n z = y-1$ (i.e., $n \notin {}^*S$). If $*N$ is effective, this procedure is effective and so $*S \cap N$ is a recursive set. It is not hard to see that $S \subseteq {}^*S \cap N$; a contradiction is reached by constructing a specific S which cannot be so extended.

Solovay's argument begins by noticing that although PT is weaker than PA, the only thing that PT lacks is the ability to "talk about" growth arguments. But, let $*N$ be any nonstandard model of PT and let $c\ \varepsilon\ {}^*N-N$ be a nonstandard integer. In the initial segment beneath c there is a submodel with enough "room" for the argument above to be carried out. To see how this can happen let

$$*N_c = \{x\varepsilon *N | \log^k c *> x \text{ for all } k\varepsilon N\}.$$

$*N_c$ is closed under polynomial time functions. For example suppose $x \varepsilon *N_c$. Then

$$\log^{k+1} c *> x, \text{ for all } k \varepsilon N$$

and so

$$\log^k c *> 2^x *> x^2.$$

Surprisingly, $*N_c$ is also a model of PT+ exponential. This follows as above: if $x \varepsilon *N_c$

$$\log^{k+2} c *> x, \text{ for all } k \varepsilon N.$$

Thus

$$\log^k c *> 2^{2^x} *> 2^x$$

implies $2^x \varepsilon *N_c$.

Continuing in this manner, it is possible to build a model $*M \subset *N$ which is closed under enough of the PA definable functions to let the proof of Tannenbaum's Theorem be carried out. But then the recursiveness of $*N$ contradicts the nonrecursiveness of $*M$.

V. Further Discussion

The results presented above show that lower bound proofs are exactly as difficult as independence proofs. This in itself leads to interesting speculations, but we feel the real force of these results lies in the link they create between the relatively new (and rather concrete) problems of computer science and some classical questions at the foundations of mathematics. We will mention just a few possibilities which ensue from such a link.

(1) It is possible that the methods of mathematical logic may help us resolve such questions as whether or not P = NP.

(2) Since lower bound proofs are equivalent to independence proofs, it is possible that the lower bound statements themselves are independent from PA or similar theorems. We make the following conjecture: "P = NP" is independent of PT.

(3) Following the measuring of (2), a viable approach to lower bounds might be to look for consistency with theories such as PA and PT.

(4) It is possible that a nontrivial lower bound will be proved, providing an entirely new method of building nonstandard models for arithmetic.

(5) It is possible that $T \vdash \Delta_S(A,B)$ implying the existence of a polynomial but quite useless algorithm for S.

(6) The main result of Section III together with Solovay's result comes very close to explaining the difficulty in obtaining lower bounds: any such proof must implicitly construct a noneffective system. This makes it seem far less likely that the finite combinatorial methods of the sort which have been applied in extant lower bound proofs will be able to prove nontrivial lower bounds are NP-complete problems.

ACKNOWLEDGEMENTS

We would like to thank Manuel Blum, David Dobkin, Stephen Kleene, Larry Landweber, Nancy Lynch, and Rick Statman for helpful conversations. A special thanks is due to Robert Solovay for sharing with us the main result of Section IV.

REFERENCES

[Ba] J. Barwise, Handbook of Mathematical Logic, North Holland, 1978.

[BL] W. Brainerd and L. Landweber, The Theory of Computation, Wiley, 1974.

[BS] J. Bell and J. Slomson, Models and Ultraproducts, North-Holland, 1970.

[Bu] J. P. Burgess, "Forcing", in [Ba], pp. 403-542.

[Co] P. J. Cohen, Set Theory and the Continuum Hypothesis, Benjamin, 1966.

[Ck1] S. Cook, "Feasibly Constructive Proofs and the Propositional Calculus", Proceedings Seventh ACM Symposium on the Theory of Computing, 1975.

[Ck2] S. Cook and R. Rechow, "On the Lengths of Proofs in the Propositional Calculus", Proceedings Sixth ACM Symposium on the Theory of Computing, 1974, pp. 135-148.

[DL] R. DeMillo and R. Lipton, "Independence", SIGACT News (to appear).

[Do] D. Dobkin and S. Reiss, "The Complexity of Linear Programming", Yale University Technical Report, No. 69, June 1978.

[EK] A. Ehrenfeucht and G. Kreisel, "Strong Models of Arithmetic", Mathematics and Logic, 1966.

[HH] J. Hartmanis and J. Hopcroft, "Independence Results in Computer Science", SIGACT News, Vol. 8, No. 4, 1976, pp. 13-23.

[Kl] S. Kleene, Introduction to Metamathematics, VanNostrand, 1953.

[Li] R. Lipton, "Model Theoretic Aspects of Computational Complexity", Proceedings 19th FOCS, 1978, pp. 193-200.

[MS] A. Meyer and L. Stockmeyer, "Nonelementary Word Problems in Automata Theory and Logic", Proceedings AMS Symposium on Complexity of Computation, 1973.

[MT] R. Miller and J. Thatcher, Complexity of Computer Computations, Plenum, 1972.

[PH] J. Paris and L. Harrington, "A Mathematical Incompleteness in Peano Arithmetic", in [Ba], pp. 1133-1142.

[Pr] V. Pratt, "Every Prime Has a Succinct Certificate", SIAM J. Computing, 1975.

[Ri] R. Rivest, private communication.

[Sc] D. S. Scott, "On Constructing Models for Arithmetic", Infinitistic Methods, Warsaw, 1959 (Oxford, 1961), pp. 235-255.

[Sh] J. Shepherdson, "Nonstandard Models of Fragments of Arithmetic", Model Theory, (J. Addison, ed.), North-Holland, 1963, pp. 342-358.

[Sk] Th. Skolem, "Uber die Nich-charakterisier barkeit der Zahlenreihe Mittels endlich oder abzahlbar unendlich vieler Aussagen mit Ausschliesslich Zahlenveriablen", Fund. Math. 23, pp. 150-161, 1934.

[Skl] Th. Skolem, "Peano's Axioms and Models of Arithmetic", Mathematical Interpretations of Formal Systems, Amsterdam, 1955, pp. 1-14.

[St] R. Statman, private communication.

[Stl] R. Statman, "Herbrand's Theorem and Gentzen's Notion of Direct Proof", in [Ba], pp. 897-912.

18 ARO

19 14690.9-EL

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER
14 GIT-ICS-79/01

2. GOVT ACCESSION NO.

3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
6 Some Connection Between Mathematical Logic and Complexity Theory

5. TYPE OF REPORT & PERIOD COVERED

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)
10 Richard A. DeMillo, Richard J. Lipton

8. CONTRACT OR GRANT NUMBER(s)
15 DAAG29-76-~~0024~~ G-0338
NSF MCS 78-81486, ~~MCS-78-07379~~
~~MCS-78-01689~~

9. PERFORMING ORGANIZATION NAME AND ADDRESS
School of Information and Computer Science
Georgia Institute of Technology
Atlanta, Georgia 30332

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS

11. CONTROLLING OFFICE NAME AND ADDRESS
12 24p.

12. REPORT DATE
11 Apr[redacted]79

13. NUMBER OF PAGES
20 + ii

14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)
US Army Research Office
PO Box 12211
Research Triangle Park, N.C. 27709

15. SECURITY CLASS. (of this report)
Unclassified

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for Published Releases; Distribution Unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

The findings of this report are not to be construed as an official Department of the Army position, unless so designated by other authorized document.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

arithmetic, complexity, logic, models, NP-completeness, nonstandard model

intersection

410 044

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The existence of lower bounds for problems in NP $\cap$ coNP is equivalent to the existence of nonstandard, noneffective models of a fragment, PT, of complete arithmetic. A typical corrollary is that factoring integers is intractable iff there is a model of arithmetic in which primes fail to have primitive roots. Following from the proof of the main result is an existential proof procedure for polynomial time algorithms.